

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

RYAN TANNER, individually and on behalf of
all others similarly situated,

Plaintiff,

v.

CONVERGENT OUTSOURCING, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Ryan Tanner and ("Plaintiff") bring this Class Action Complaint against Convergent Outsourcing, Inc. ("Convergent" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters, as follows:

1. Defendant Convergent is a large third-party debt collector company with its primary place of business located in Renton, Washington. As part of Defendant's business, Convergent acquires, stores, processes, analyzes, and otherwise utilizes for its business purposes personally identifiable information ("PII" or "Private Information"), including first and last names, contact information, financial account numbers, and Social Security numbers.

2. Plaintiff and Class Members are individuals whose Private Information was acquired, stored, and utilized by Defendant for its business and financial benefit.

1 3. By obtaining, collecting, utilizing, and deriving a benefit from Plaintiff's and Class
2 Members' Private Information, Defendant owed and otherwise assumed statutory, regulatory,
3 contractual, and common law duties and obligations to keep Plaintiff's and Class Members'
4 Private Information confidential, safe, secure, and protected from the unauthorized access,
5 disclosure, and theft in foreseeable data breach incidents.

6 4. Defendant, however, disregarded its duties and obligations and the privacy
7 rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently
8 failing to take and implement adequate and reasonable data security measures to protect and
9 safeguard the Private Information of Plaintiff and Class Members, but rather allowed the
10 Private Information to be stored and maintained in a vulnerable state.

11 5. As a result of Defendant's failure to implement and maintain reasonable data
12 security measures, an external actor was able to gain unauthorized access to Defendant's
13 systems and deploy a ransomware malware. The unauthorized actor was able to deploy certain
14 data extraction tools, allowing the actor to access, exfiltrate, and steal the Private Information
15 of Plaintiff and Class Members (the "Data Breach"). But for Defendant's acts and omissions, the
16 Data Breach would not have happened, and Plaintiff and Class Members would not have been
17 injured as described herein.

18 6. Defendant admits in notice letters to Plaintiff and Class Members that the
19 Private Information impacted during the Data Breach included at least names, contact
20 information, financial account numbers, and Social Security numbers.

21 7. The exposed Private Information of Plaintiff and Class Members is highly
22 sensitive and utilized to commit identity theft and fraud. The Private Information has been or
23 likely will be sold on the dark web, as this is the modus operandi for cyber criminals targeting
24 this type of Private Information. Plaintiff and Class Members, therefore, are now at a current
25 and ongoing risk of identity theft, which is heightened here by the theft of their Social Security
26 numbers – the gold standard for identity thieves.
27

8. While many details of the Data Breach remain in the exclusive control of Defendant, upon information and belief, Defendant breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train employees on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that an unauthorized actor had accessed its network in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent ransomware, and (9) otherwise failing to secure Defendant's network using reasonable and effective data security procedures free of foreseeable vulnerabilities.

9. Moreover, despite learning of the Data Breach in June 2022, Defendant did not begin notifying Plaintiff and Class Members until approximately October 26, 2022.

10. As a result of Defendant's acts and omissions, Plaintiff and Class Members had their most sensitive Private Information stolen by malicious cybercriminals. The information that was compromised is a one-stop shop for identity thieves to wreak havoc on Plaintiff's and Class Members' personal and financial lives. Given the sensitivity and static nature of the information involved (such as names and Social Security numbers), the risk of identity theft is present, materialized, and will continue into the foreseeable future for Plaintiff and Class Members.

11. As a direct result of the Data Breach, Plaintiff and Class Members have suffered the following actual and imminent injuries: (i) invasion of privacy; (ii) out-of-pocket expenses; (iii) loss of time and productivity incurred mitigating the present risk and imminent threat of identity theft; (iv) actual identity theft and fraud resulting in additional economic and non-economic damages; (v) diminution of value of their PII; (vi) anxiety, stress, nuisance, and annoyance; (vii) the present and continuing risk of identity theft posed by their Private

Information being placed in the hands of the ill-intentioned hackers and/or criminals; (ix) the retention of the reasonable value of the Private Information entrusted to Defendant; and (x) the present and continued risk to Private Information, which remains on Defendant's vulnerable network, placing Plaintiff and Class Members at an ongoing risk of harm.

12. Plaintiff brings this class action to remedy these harms, on behalf of themselves and all similarly situated persons whose Private Information was compromised in the Data Breach. Plaintiff seeks compensatory damages, incidental damages, and consequential damages for the diminution in value of their PII, invasion of their privacy, loss of their time, loss of their productivity, out-of-pocket costs, and future costs of necessary identity theft monitoring. Plaintiff also seeks injunctive relief including improvements to Defendant's data security system and protocols, deletion of Private Information that is unnecessary for legitimate business purposes, and future annual audits to protect their Private Information against foreseeable future cyber security incidents.

13. Plaintiff brings this Class Action Complaint against Defendant asserting claims for: (1) negligence, (2) breach of implied contract, (3) unjust enrichment, and (4) declaratory judgment/injunctive relief.

I. PARTIES

14. Plaintiff Ryan Tanner is a resident and citizen of Minnesota, residing in Cambridge, Minnesota. Plaintiff Tanner received a Notice of Data Security Incident letter from Convergent, dated October 26, 2022, by U.S. Mail.

15. Defendant Convergent Outsourcing, Inc., is a corporation with its principal place of business located at 800 SW 39th Street, Suite 100, Renton, WA 98057.

II. JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs; there are more than 100 members in the

1 proposed class; and at least one member of the class, including the Plaintiff, are citizens of a
2 state different from Defendant.

3 17. This Court has personal jurisdiction over Defendant because its principal place of
4 business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in
5 and emanated from this District.

6 18. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place
7 of business is in this District and a substantial part of the events or omissions giving rise to
8 Plaintiff's claims occurred in this District.

9 III. FACTUAL ALLEGATIONS

10 19. Defendant Convergent boasts that it is one of "America's leading collection
11 agencies with offices across the country."¹ For more than sixty years, Covergent has worked
12 with clients in process outsourcing, revenue cycle and receivables management.²

13 ***Convergent Collects Private Information***

14 20. Defendant collects the Private Information of its clients' customers as a
15 condition of providing services. This Private Information is used by Defendant in the ordinary
16 course of its business to, *inter alia*, collect debts. At the time of the Data Breach, Defendant
17 provided services to a number of different clients in the telecommunications, utilities, banking,
18 cable, and financial industries.³

19 21. The types of private information collected and utilized by Defendant includes, at
20 least, names, contact information, financial information, and Social Security numbers.

21
22
23
24
25 ¹ <https://www.convergentusa.com/outsourcing/site/who-is-convergent-outsourcing> (last
26 visited Nov. 2, 2022).

27 ² *Id.*

³ <https://www.convergentusa.com/outsourcing/question/list?type=A> (last visited Nov. 2, 2022).

Defendant's Privacy Policy & Promises

22. On its customer-facing website, Defendant has a posted Privacy Policy, last updated July 16, 2020 (the "Privacy Policy").⁴

23. Defendant's Privacy Policy pertains to Private Information provided to Defendant and any Private Information that Defendant collects through an individual's online activity, including use of Defendant's Payment Portal.⁵

24. The Privacy Policy discusses the types of information Convergent collects and the reasons that it might use that information. Defendant lists a number of instances when it might share or disclose the Private Information entrusted to it without permission, none of which are applicable here.⁶

The Data Breach

25. According to Convergent, on June 17, 2022, it became aware of an interruption to certain services performed by Convergent affecting certain computer systems. Upon investigation, Convergent determined that an external actor gained unauthorized access to its systems and deployed a ransomware malware.⁷

26. According to Convergent, its subsequent investigation determined that "the unauthorized actor deployed certain data extraction tools on one storage drive that is used to save and share files internally."⁸

27. The investigation further revealed that the following Private Information was involved in the unauthorized access of the internal drive: names, contact information, financial account numbers, and Social Security numbers.

⁴ <https://www.convergentusa.com/outsourcing/page/privacy-policy> (last accessed Nov. 2, 2022).

⁵ *Id.*

⁶ *See id.*

⁷ Exhibit 1, Notice of Data Breach Letter

⁸ *Id.*

28. On October 26, 2022, over four months after Convergent first discovered the Data Breach, Convergent finally notified Plaintiff and Class Members via a Notice of Data Breach Letter. In the Notice of Data Breach Letter, Convergent instructed Plaintiff and Class Members to “remain vigilant and monitor your account statements, insurance transactions, and free credit reports for potential fraud and identity theft, and promptly report any concerns.”⁹

29. Convergent reprehensibly downplayed the risk faced by Plaintiff and Class Members by publicly stating that Convergent’s investigation, which was clearly insufficient, “could not confirm [Plaintiff’ and Class Members’] personally information was *actually* viewed by the unauthorized actor.”¹⁰.

The Data Breach was Foreseeable and Preventable

30. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”¹¹

31. Defendant has not publicly shared details of the Data Breach. However, based on Defendant’s limited statements, it is clear Defendant did not take reasonable precautions that would have allowed it to quickly detect, prevent, stop, undo, or remediate the effects of the Data Breach. These failures allowed cybercriminals using well publicized attack practices to access and steal the Private Information Defendant maintained on Plaintiff and Class Members.

32. Defendant could have prevented the Data Breach by encrypting the systems and files containing the Private Information of Plaintiff and Class Members and by destroying Private Information it no longer had a legitimate need for.

33. Additionally, to prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures known to be generally effective at mitigating the risk of a cyberattack:

⁹ *Id.*

¹⁰ *Id.*

¹¹ See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Aug. 23, 2021).

- 1 • Implement an awareness and training program. Because end users are
- 2 targets, employees and individuals should be aware of the threat of
- 3 ransomware and how it is delivered.
- 4 • Enable strong spam filters to prevent phishing emails from reaching the
- 5 end users and authenticate inbound email using technologies like Sender
- 6 Policy Framework (SPF), Domain Message Authentication Reporting and
- 7 Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to
- 8 prevent email spoofing.
- 9 • Scan all incoming and outgoing emails to detect threats and filter
- 10 executable files from reaching end users.
- 11 • Configure firewalls to block access to known malicious IP addresses.
- 12 • Patch operating systems, software, and firmware on devices. Consider
- 13 using a centralized patch management system.
- 14 • Set anti-virus and anti-malware programs to conduct regular scans
- 15 automatically.
- 16 • Manage the use of privileged accounts based on the principle of least
- 17 privilege: no users should be assigned administrative access unless
- 18 absolutely needed; and those with a need for administrator accounts
- 19 should only use them when necessary.
- 20 • Configure access controls—including file, directory, and network share
- 21 permissions—with least privilege in mind. If a user only needs to read
- 22 specific files, the user should not have write access to those files,
- 23 directories, or shares.
- 24 • Disable macro scripts from office files transmitted via email. Consider
- 25 using Office Viewer software to open Microsoft Office files transmitted
- 26 via email instead of full office suite applications.
- 27

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹²

34. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks. . . .
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the

¹² See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Nov. 2, 2022).

sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net). . . .

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it. . . .
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. . . .¹³

¹³ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited Aug. 23, 2022).

35. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹⁴

36. Given that Defendant was storing the Private Information of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

37. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the unauthorized exposure and exfiltration of the Private Information of Plaintiff and Class Members.

38. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

39. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

Value of Private Information

40. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."¹⁵ The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."¹⁶

¹⁴ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Aug. 23, 2022).

¹⁵ 17 C.F.R. § 248.201 (2013).

¹⁶ *Id.*

41. PII is inherently valuable and the frequent target of hackers. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.¹⁷

42. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.¹⁸ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.¹⁹ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²⁰

43. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items

¹⁷ See *2021 Data Breach Annual Report* (ITRC, Jan. 2022), available at <https://notified.idtheftcenter.org/s/>, at 6.

¹⁸ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Oct. 27, 2022).

¹⁹ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Oct. 27, 2021).

²⁰ *In the Dark*, VPNOOverview, 2019, available at <https://vpnooverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Oct. 27, 2021).

1 you never bought. Someone illegally using your Social Security
2 number and assuming your identity can cause a lot of problems.²¹

3 44. What is more, it is no easy task to change or cancel a stolen Social Security
4 number. An individual cannot obtain a new Social Security number without significant
5 paperwork and evidence of actual misuse. In other words, preventive action to defend against
6 the possibility of misuse of a Social Security number is not permitted; an individual must show
7 evidence of actual, ongoing fraud activity to obtain a new number.

8 45. Even then, a new Social Security number may not be effective. According to Julie
9 Ferguson of the Identity Theft Resource Center, “The credit bureaus and banks are able to link
10 the new number very quickly to the old number, so all of that old bad information is quickly
11 inherited into the new Social Security number.”²²

12 46. Based on the foregoing, the Private Information compromised in the Data Breach
13 is significantly more valuable than the loss of, for example, credit card information in a retailer
14 data breach because, there, victims can cancel or close credit and debit card accounts. The
15 Information compromised in this Data Breach is impossible to “close” and difficult, if not
16 impossible, to change: Social Security number and name.

17 47. This data demands a much higher price on the black market. Martin Walter,
18 senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information,
19 personally identifiable information and Social Security numbers are worth more than 10x on
20 the black market.”²³

21
22 ²¹ Social Security Administration, *Identity Theft and Your Social Security Number*, available at
23 <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Oct. 27, 2021).

24 ²² Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb.
25 9, 2015), available at [http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-](http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft)
26 hackers-has-millionsworrying-about-identity-theft (last visited Oct. 27, 2021).

27 ²³ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*
 Numbers, IT World, (Feb. 6, 2015), available at
 [https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-](https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html)
 10x-price-of-stolen-credit-card-numbers.html (last visited Aug. 23, 2021).

1 48. Among other forms of fraud, identity thieves may obtain driver's licenses,
2 government benefits, medical services, and housing, or even give false information to police.

3 49. The fraudulent activity resulting from the Data Breach may not come to light for
4 years.

5 50. Moreover, there may be a time lag between when harm occurs versus when it is
6 discovered, and also between when Private Information is stolen and when it is used. According
7 to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data
8 breaches:

9 [L]aw enforcement officials told us that in some cases, stolen data
10 may be held for up to a year or more before being used to commit
11 identity theft. Further, once stolen data have been sold or posted
12 on the Web, fraudulent use of that information may continue for
13 years. As a result, studies that attempt to measure the harm
14 resulting from data breaches cannot necessarily rule out all future
15 harm.²⁴

16 51. At all relevant times, Defendant knew, or reasonably should have known, of the
17 importance of safeguarding the Private Information of Plaintiff and Class Members, including
18 Social Security numbers, and of the foreseeable consequences that would occur if Defendant's
19 data security system was breached, including, specifically, the significant costs that would be
20 imposed on Plaintiff and Class Members as a result of a breach.

21 52. The ramifications of Defendant's failure to keep secure the Private Information
22 of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen,
23 particularly Social Security numbers, fraudulent use of that information and damage to victims
24 may continue for years. Plaintiff and Class Members now face years of constant surveillance of
25 their financial and personal records, monitoring, and loss of rights. The Class is incurring and
26 will continue to incur such damages, in addition to any fraudulent use of their Private
27 Information.

²⁴ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at
<https://www.gao.gov/assets/gao-07-737.pdf> (last visited Aug. 23, 2021).

53. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

54. To date, Defendant has offered Plaintiff and Class Members only 12 months of credit monitoring services through IDX. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the Private Information at issue here. Moreover, Defendant put the burden squarely on Plaintiff and Class Members to enroll in the inadequate monitoring services that it offered.

55. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

56. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

57. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

58. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and purposes, and to prevent the unauthorized disclosures of the Private Information.

Defendant Failed to Comply with FTC Guidelines

59. Defendant was prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an

1 “unfair practice” in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799
2 F.3d 236 (3d Cir. 2015).

3 60. The Federal Trade Commission (“FTC”) has promulgated numerous guides for
4 businesses that highlight the importance of implementing reasonable data security practices.
5 According to the FTC, the need for data security should be factored into all business decision-
6 making.²⁵

7 61. In 2016, the FTC updated its publication, *Protecting Personal Information: A*
8 *Guide for Business*, which established cybersecurity guidelines for businesses.²⁶ The guidelines
9 note that businesses should protect the personal customer information that they keep;
10 properly dispose of personal information that is no longer needed; encrypt information stored
11 on computer networks; understand their network’s vulnerabilities; and implement policies to
12 correct any security problems.

13 62. The FTC further recommends that companies not maintain PII longer than is
14 needed for authorization of a transaction; limit access to private data; require complex
15 passwords to be used on networks; use industry-tested methods for security; monitor for
16 suspicious activity on the network; and verify that third-party service providers have
17 implemented reasonable security measures.²⁷

18 63. The FTC has brought enforcement actions against businesses for failing to
19 adequately and reasonably protect customer data, treating the failure to employ reasonable
20 and appropriate measures to protect against unauthorized access to confidential consumer
21 data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders
22

23 ²⁵ FEDERAL TRADE COMMISSION, *Start With Security: A Guide for Business*, available at
24 <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>
25 (last visited July 7, 2022).

26 ²⁶ FEDERAL TRADE COMMISSION, *Protecting Personal Information: A Guide for Business*, available at
27 [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)
information.pdf (last visited July 7, 2022).

²⁷ FTC, *Start With Security*, *supra*.

1 resulting from these actions further clarify the measures businesses must take to meet their
2 data security obligations.

3 64. Defendant failed to properly implement basic data security practices.
4 Defendant's failure to employ reasonable and appropriate measures to protect against
5 unauthorized access to Plaintiff' and Class Members' Private Information constitutes an unfair
6 act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

7 65. Defendant was at all times fully aware of its obligation to protect the PII stored
8 within its systems because of its position as a leading business affiliate to a variety of
9 companies. Defendant was also aware of the significant repercussions that would result from
10 its failure to do so.

11 ***Plaintiff Tanner's Experiences***

12 66. Prior to the Data Breach, Defendant retained Plaintiff Tanner's name, contact
13 information, financial information, and Social Security number.

14 67. Plaintiff Tanner provided his Private Information directly to one of Defendant's
15 clients and indirectly to Defendant with the expectation that his Private Information would
16 remain confidential.

17 68. Plaintiff Tanner trusted that his Private Information would be safeguarded
18 according to internal policies and state and federal law.

19 69. Upon information and belief, Plaintiff Tanner's Private Information was stored
20 on Defendant's network during the Data Breach and presently remains in Defendant's
21 possession.

22 70. On approximately October 26, 2022, Defendant notified Plaintiff Tanner that
23 Defendant's network had been accessed by an unauthorized actor and that Plaintiff Tanner's
24 Private Information may have been involved in the Data Breach.

25 71. Plaintiff Tanner is very careful about sharing his sensitive Private Information.
26 Plaintiff Tanner has never knowingly transmitted unencrypted sensitive Private Information
27

1 over the internet or any other unsecured source. Plaintiff Tanner stores any documents
2 containing his Private Information in a safe and secure location or destroys the documents.

3 72. As a result of the Data Breach, Plaintiff Tanner has spent time dealing with the
4 consequences of the Data Breach, which include time spent verifying the legitimacy of the
5 Notice of Data Breach Letter, and self-monitoring his accounts and credit reports to ensure no
6 fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

7 73. Plaintiff Tanner suffered actual injury in the form of damages to and diminution
8 in the value of Plaintiff Tanner's Private Information—a form of intangible property that
9 Plaintiff Tanner entrusted to Defendant—which was compromised in and as a result of the Data
10 Breach.

11 74. Additionally, Plaintiff Tanner suffered actual injury in the form of fraudulent
12 charges on his financial accounts. Specifically, since the Data Breach, Plaintiff Tanner was made
13 aware of unauthorized charges for Netflix in the amount of approximately \$100. Plaintiff
14 Tanner, who was unemployed at the time the charges went through, spent several hours
15 attempting to dispute the fraudulent charges with his bank and was forced to borrow money
16 while the charges were being disputed.

17 75. Plaintiff Tanner suffered lost time, annoyance, interference, and inconvenience
18 as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

19 76. Plaintiff Tanner has suffered imminent and impending injury arising from the
20 substantially increased risk of fraud, identity theft, and misuse resulting from his Private
21 Information being placed in the hands of unauthorized third parties and possibly criminals.

22 77. Plaintiff Tanner has a continuing interest in ensuring that his Private
23 Information—which, upon information and belief, remains backed up in Defendant's
24 possession—is protected and safeguarded from future breaches.

IV. CLASS ALLEGATIONS

78. Plaintiff brings this nationwide class action on behalf of himself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

79. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

All United States residents whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach Letter that Defendant sent to Plaintiff and other Class Members on or around October 26, 2022

80. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

81. Plaintiff reserves the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

82. Numerosity, Fed. R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds of thousands, if not millions, of individuals whose Private Information may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

83. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

- 1 b. Whether Defendant had duties not to disclose the Private Information of
2 Plaintiff and Class Members to unauthorized third parties;
- 3 c. Whether Defendant had duties not to use the Private Information of
4 Plaintiff and Class Members for non-business purposes;
- 5 d. Whether Defendant failed to adequately safeguard the Private
6 Information of Plaintiff and Class Members;
- 7 e. Whether and when Defendant actually learned of the Data Breach;
- 8 f. Whether Defendant adequately, promptly, and accurately informed
9 Plaintiff and Class Members that their Private Information had been
10 compromised;
- 11 g. Whether Defendant violated the law by failing to promptly notify Plaintiff
12 and Class Members that their Private Information had been
13 compromised;
- 14 h. Whether Defendant failed to implement and maintain reasonable
15 security procedures and practices appropriate to the nature and scope of
16 the information compromised in the Data Breach;
- 17 i. Whether Defendant adequately addressed and fixed the vulnerabilities
18 that permitted the Data Breach to occur;
- 19 j. Whether Plaintiff and Class Members are entitled to actual, incidental,
20 consequential, and/or nominal damages as a result of Defendant's
21 wrongful conduct;
- 22 k. Whether Plaintiff and Class Members are entitled to restitution as a
23 result of Defendant's wrongful conduct; and
- 24 l. Whether Plaintiff and Class Members are entitled to injunctive relief to
25 redress the imminent and currently ongoing harm faced as a result of the
26 Data Breach.
27

1 84. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other
2 Class Members because all had their Private Information compromised as a result of the Data
3 Breach due to Defendant's misfeasance.

4 85. Policies Generally Applicable to the Class: This class action is also appropriate for
5 certification because Defendant has acted or refused to act on grounds generally applicable to
6 the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible
7 standards of conduct toward the Class Members and making final injunctive relief appropriate
8 with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect
9 Class Members uniformly, and Plaintiff's challenge of these policies hinges on Defendant's
10 conduct with respect to the Class as a whole, not on facts or law applicable only to an individual
11 Plaintiff.

12 86. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent
13 and protect the interests of the Class Members in that Plaintiff have no disabling conflicts of
14 interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks
15 no relief that is antagonistic or adverse to the Members of the Class, and the infringement of
16 the rights and the damages Plaintiff have suffered are typical of other Class Members. Plaintiff
17 has also retained counsel experienced in complex class action litigation, and Plaintiff intends to
18 prosecute this action vigorously.

19 87. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an
20 appropriate method for fair and efficient adjudication of the claims involved. Class action
21 treatment is superior to all other available methods for the fair and efficient adjudication of the
22 controversy alleged herein; it will permit a large number of Class Members to prosecute their
23 common claims in a single forum simultaneously, efficiently, and without the unnecessary
24 duplication of evidence, effort, and expense that hundreds of individual actions would require.
25 Class action treatment will permit the adjudication of relatively modest claims by certain Class
26 Members, who could not individually afford to litigate a complex claim against large
27 corporations, like Defendant. Further, even for those Class Members who could afford to

1 litigate such a claim, it would still be economically impractical and impose a burden on the
2 courts.

3 88. The nature of this action and the nature of laws available to Plaintiff and Class
4 Members make the use of the class action device a particularly efficient and appropriate
5 procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because
6 Defendant would necessarily gain an unconscionable advantage since they would be able to
7 exploit and overwhelm the limited resources of each individual Class Member with superior
8 financial and legal resources; the costs of individual suits could unreasonably consume the
9 amounts that would be recovered; proof of a common course of conduct to which Plaintiff
10 were exposed is representative of that experienced by the Class and will establish the right of
11 each Class Member to recover on the cause of action alleged; and individual actions would
12 create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

13 89. The litigation of the claims brought herein is manageable. Defendant's uniform
14 conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class
15 Members demonstrates that there would be no significant manageability problems with
16 prosecuting this lawsuit as a class action.

17 90. Adequate notice can be given to Class Members directly using information
18 maintained in Defendant's records.

19 91. Unless a Class-wide injunction is issued, Defendant may continue in its failure to
20 properly secure the Private Information of Class Members, Defendant may continue to refuse
21 to provide proper notification to Class Members regarding the Data Breach, and Defendant may
22 continue to act unlawfully as set forth in this Complaint.

23 92. Further, Defendant has acted or refused to act on grounds generally applicable
24 to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to
25 the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil
26 Procedure.
27

1 93. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification
 2 because such claims present only particular, common issues, the resolution of which would
 3 advance the disposition of this matter and the parties' interests therein. Such particular issues
 4 include, but are not limited to:

- 5 a. Whether Defendant owed a legal duty to Plaintiff and Class Members to
- 6 exercise due care in collecting, storing, using, and safeguarding their
- 7 Private Information;
- 8 b. Whether Defendant breached a legal duty to Plaintiff and Class Members
- 9 to exercise due care in collecting, storing, using, and safeguarding their
- 10 Private Information;
- 11 c. Whether Defendant failed to comply with its own policies and applicable
- 12 laws, regulations, and industry standards relating to data security;
- 13 d. Whether an implied contract existed between Defendant on the one
- 14 hand, and Plaintiff and Class Members on the other, and the terms of
- 15 that implied contract;
- 16 e. Whether Defendant breached the implied contract;
- 17 f. Whether Defendant adequately and accurately informed Plaintiff and
- 18 Class Members that their Private Information had been compromised;
- 19 g. Whether Defendant failed to implement and maintain reasonable
- 20 security procedures and practices appropriate to the nature and scope of
- 21 the information compromised in the Data Breach;
- 22 h. Whether Class Members are entitled to actual, consequential, and/or
- 23 nominal damages, and/or injunctive relief as a result of Defendant's
- 24 wrongful conduct.

V. CAUSES OF ACTION

COUNT I

NEGLIGENCE

(On Behalf of Plaintiff and the Nationwide Class)

94. Plaintiff repeats and re-alleges each and every allegation in the Complaint as if fully set forth herein.

95. Plaintiff and the Class entrusted Defendant with their Private Information.

96. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

97. Defendant has full knowledge and had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

98. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

99. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiff and the Class in Defendant's possession was adequately secured and protected.

100. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain pursuant to regulations.

101. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiff and the Class.

1 102. Defendant's duty to use reasonable security measures arose as a result of the
2 special relationship that existed between Defendant and Plaintiff and the Class. That special
3 relationship arose because Plaintiff and the Class entrusted Defendant with their confidential
4 Private Information, a necessary part of obtaining services from Defendant. That duty further
5 arose because Defendant chose to collect and maintain the Private Information for its own
6 pecuniary benefit.

7 103. Defendant was subject to an "independent duty," untethered to any contract
8 between Defendant and Plaintiff or the Class.

9 104. A breach of security, unauthorized access, and resulting injury to Plaintiff and the
10 Class was reasonably foreseeable, particularly in light of Defendant's inadequate security
11 practices.

12 105. Plaintiff's and the Class's injuries were the foreseeable and probable result of
13 any inadequate security practices and procedures. Defendant knew or should have known of
14 the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the
15 critical importance of providing adequate security of that Private Information, and the necessity
16 for encrypting Private Information stored on Defendant's systems.

17 106. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the
18 Class. Defendant's misconduct included, but was not limited to, their failure to take the steps
19 and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also
20 included their decisions not to comply with industry standards for the safekeeping of the
21 Private Information of Plaintiff and the Class, including basic encryption techniques freely
22 available to Defendant.

23 107. Plaintiff and the Class had no ability to protect their Private Information that was
24 within, and on information and belief remains within, Defendant's possession.

25 108. Defendant was in a position to protect against the harm suffered by Plaintiff and
26 the Class as a result of the Data Breach.
27

1 109. Defendant had (and continues to have) a duty to adequately disclose that the
2 Private Information of Plaintiff and the Class within Defendant's possession might have been
3 compromised, how it was compromised, and precisely the types of data that were
4 compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps
5 to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private
6 Information by third parties.

7 110. Defendant had a duty to employ proper procedures to prevent the unauthorized
8 dissemination of the Private Information of Plaintiff and the Class.

9 111. Defendant, through its actions and/or omissions, unlawfully breached its duties
10 to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable
11 care in protecting and safeguarding the Private Information of Plaintiff and the Class during the
12 time the Private Information was within Defendant's possession or control.

13 112. Defendant improperly and inadequately safeguarded the Private Information of
14 Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the
15 time of the Data Breach.

16 113. Defendant failed to heed industry warnings and alerts to provide adequate
17 safeguards to protect the Private Information of Plaintiff and the Class in the face of increased
18 risk of theft.

19 114. Defendant, through its actions and/or omissions, unlawfully breached its duty to
20 Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent
21 dissemination of Private Information.

22 115. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff
23 and the Class, the Private Information of Plaintiff and the Class would not have been
24 compromised.

25 116. There is a close causal connection between Defendant's failure to implement
26 adequate data security measures to protect the Private Information of Plaintiff and the Class
27 and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private

1 Information of Plaintiff and the Class was lost and accessed as the proximate result of
2 Defendant's failure to exercise reasonable care in safeguarding such Private Information by
3 adopting, implementing, and maintaining appropriate security measures.

4 117. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or
5 affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or
6 practice by businesses, such as Defendant, of failing to use reasonable measures to protect
7 Private Information. The FTC publications and orders described above also form part of the
8 basis of Defendant's duty in this regard.

9 118. Defendant violated Section 5 of the FTC Act by failing to use reasonable
10 measures to protect Private Information and by not complying with applicable industry
11 standards, as described in detail herein. Defendant's conduct was particularly unreasonable
12 given the nature and amount of Private Information it obtained and stored and the foreseeable
13 consequences of the immense damages that would result to Plaintiff and the Class.

14 119. Defendant's violation of Section 5 of the FTC Act is, in and of itself, evidence of
15 Defendant's negligent data security practices.

16 120. Plaintiff and the Class are within the class of persons that the FTC Act was
17 intended to protect.

18 121. The harm that occurred as a result of the Data Breach is the type of harm the
19 FTC Act was intended to guard against. The FTC has pursued enforcement actions against
20 businesses, which, as a result of their failure to employ reasonable data security measures and
21 avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the
22 Class.

23 122. As a direct and proximate result of Defendant's negligence, Plaintiff and the
24 Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft;
25 (ii) the loss of the opportunity to decide how their Private Information is used; (iii) the
26 compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses
27 associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or

1 unauthorized use of their Private Information; (v) lost opportunity costs associated with effort
 2 expended and the loss of productivity addressing and attempting to mitigate the present and
 3 continuing consequences of the Data Breach, including but not limited to efforts spent
 4 researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi)
 5 costs associated with placing freezes on credit reports; (vii) the continued risk to their Private
 6 Information, which remains in Defendant's possession and is subject to further unauthorized
 7 disclosures so long as Defendant fails to undertake appropriate and adequate measures to
 8 protect the Private Information of Plaintiff and the Class; and (viii) present and continuing costs
 9 in terms of time, effort, and money that has been and will be expended to prevent, detect,
 10 contest, and repair the impact of the Private Information compromised as a result of the Data
 11 Breach for the remainder of the lives of Plaintiff and the Class.

12 123. As a direct and proximate result of Defendant's negligence, Plaintiff and the
 13 Class have suffered and will continue to suffer other forms of injury and/or harm, including, but
 14 not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-
 15 economic losses.

16 124. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff
 17 and the Class have suffered and will suffer the continued risks of exposure of their Private
 18 Information, which remains in Defendant's possession and is subject to further unauthorized
 19 disclosures so long as Defendant continues to fail to undertake appropriate and adequate data
 20 security measures to protect the Private Information in its continued possession.

21 125. As a direct and proximate result of Defendant's negligence, Plaintiff and the
 22 Class are entitled to recover actual, consequential, and nominal damages.

23 **COUNT II**
 24 **BREACH OF IMPLIED CONTRACT**
 25 **(On Behalf of Plaintiff and the Nationwide Class)**

26 126. Plaintiff repeats and re-alleges each and every allegation in the Complaint as if
 27 fully set forth herein.

1 127. Defendant required Plaintiff and the Class to provide and entrust their Private
2 Information, including, without limitation, first and last name, contact information, financial
3 account numbers, and Social Security numbers.

4 128. Defendant solicited and invited Plaintiff and the Class to provide their Private
5 Information to Defendant, either directly or indirectly through Defendant's clients, as part of
6 Defendant's regular business practices. Plaintiff and the Class accepted Defendant's offers and
7 provided their Private Information to Defendant.

8 129. As a condition of obtaining care and/or services from Defendant's clients,
9 Plaintiff and the Class provided and entrusted Defendant with their Private Information. In so
10 doing, Plaintiff and the Class entered into implied contracts with Defendant by which
11 Defendant agreed to safeguard and protect such information, to keep such information secure
12 and confidential, and to timely and accurately notify Plaintiff and the Class if their data had
13 been breached and compromised or stolen.

14 130. A meeting of the minds occurred when Plaintiff and the Class agreed to, and did,
15 provide their Private Information to Defendant and/or Defendant's clients with the reasonable
16 understanding that their Private Information would be adequately protected from foreseeable
17 threats. This inherent understanding exists independent of any other law or contractual
18 obligation any time that highly sensitive PII exchanged as a condition of receiving services. It is
19 common sense that but for this implicit and/or explicit agreement, Plaintiff and Class Members
20 would not have provided their Private Information.

21 131. Defendant separately has contractual obligations arising from and/or supported
22 by the consumer facing statements in its Privacy Policies.

23 132. Plaintiff and the Class fully performed their obligations under the implied
24 contracts with Defendant.

25 133. Defendant breached the implied contracts it made with Plaintiff and the Class by
26 failing to safeguard and protect their Private Information and by failing to provide timely and
27 accurate notice that Private Information was compromised as a result of the Data Breach.

134. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

135. As a result of Defendant's breach of implied contract, Plaintiff and the Class are entitled to and demand actual, consequential, and nominal damages.

COUNT III
UNJUST ENRICHMENT

(On behalf of Plaintiff and the Nationwide Class)

136. Plaintiff repeats and re-alleges each and every allegation in the Complaint as if fully set forth herein.

137. Plaintiff and Class Members conferred a monetary benefit on Defendant by providing Defendant, directly or indirectly, with their valuable Private Information.

138. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff' and Class Members' Private Information.

139. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

140. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members

1 because Defendant failed to implement appropriate data management and security measures
2 that are mandated by industry standards.

3 141. Defendant acquired the monetary benefit and Private Information through
4 inequitable means in that it failed to disclose the inadequate security practices previously
5 alleged.

6 142. If Plaintiff and Class Members knew that Defendant had not secured their Private
7 Information, they would not have agreed to provide their Private Information to Defendant.

8 143. Plaintiff and Class Members have no adequate remedy at law.

9 144. As a direct and proximate result of Defendant's conduct, Plaintiff and Class
10 Members have suffered and will suffer injury, including but not limited to: (i) actual identity
11 theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise,
12 publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated
13 with the prevention, detection, and recovery from identity theft, and/or unauthorized use of
14 their Private Information; (v) lost opportunity costs associated with effort expended and the
15 loss of productivity addressing and attempting to mitigate the actual and future consequences
16 of the Data Breach, including but not limited to efforts spent researching how to prevent,
17 detect, contest, and recover from identity theft; (vi) the continued risk to their Private
18 Information, which remains in Defendant's possession and is subject to further unauthorized
19 disclosures so long as Defendant fails to undertake appropriate and adequate measures to
20 protect Private Information in their continued possession and (vii) future costs in terms of time,
21 effort, and money that will be expended to prevent, detect, contest, and repair the impact of
22 the Private Information compromised as a result of the Data Breach for the remainder of the
23 lives of Plaintiff and Class Members.

24 145. As a direct and proximate result of Defendant's conduct, Plaintiff and Class
25 Members have suffered and will continue to suffer other forms of injury and/or harm.
26
27

146. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them.

COUNT IV
VIOLATION OF WASHINGTON CONSUMER PROTECTION ACT
(On Behalf of Plaintiff and the Nationwide Class)

147. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

148. Defendant is a “person” within the meaning of the Washington Consumer Protection Act, RCW 19.86.010 and it conducts “trade” and “commerce” within the meaning of RCW 19.86.010(2).

149. Plaintiff and Class Members are “persons” within the meaning of RCW 19.86.010(1).

150. Defendant engaged in unfair or deceptive acts or practices in the conduct of its business by the conduct set forth above. These unfair or deceptive acts or practices include the following:

- a. Failing to adequately secure Plaintiff’s and Class Members’ personal information from disclosure to unauthorized third parties or for improper purposes;
- b. Enabling the disclosure of personal and sensitive facts about Plaintiff and the Class in a manner highly offensive to the reasonable person;
- c. Enabling the disclosure of personal and sensitive facts about Plaintiff and the Class without their informed, voluntary, affirmative, and clear consent;
- d. Omitting, suppressing, and concealing the material fact that Defendant did not reasonably or adequately secure Plaintiff’s and Class Members’ personal information; and
- e. Failing to disclose the data breach in a timely and accurate manner.

1 151. Defendant's systematic acts or practices are unfair because the acts or practices
2 are immoral, unethical, oppressive, and/or unscrupulous.

3 152. Defendant's systematic acts or practices are deceptive because they were and
4 are capable of deceiving a substantial portion of the public.

5 153. Defendant's unfair or deceptive acts or practices have repeatedly occurred in
6 trade of commerce within the meaning of RCW 19.86.010 and RCW 19.86.020.

7 154. The acts complained herein are ongoing and/or have substantial likelihood of
8 being repeated.

9 155. Defendant's unfair or deceptive acts or practices impact the public interest
10 because they have injured Plaintiff and Washington citizens and have the capacity to injure
11 thousands more.

12 156. As a direct and proximate result of Defendant's unfair or deceptive acts or
13 practices, Plaintiff and Class Members have suffered injury in fact and lost money.

14 157. As a result of Defendant's conduct, Plaintiff and Class Members have suffered
15 actual damages including, without limitation, time and expenses related to monitoring their
16 financial accounts for fraudulent activity, an increased and imminent risk of fraud and identity
17 theft, the lost value of their personal information, and other economic and non-economic
18 harm.

19 158. Plaintiff and Class Members are therefore entitled to legal relief, including
20 recovery of actual damages, treble damages, attorneys' fees and costs, and such further relief as
21 the Court may deem proper.

22 159. Plaintiff and Class Members are also entitled to injunctive relief in the form of an
23 order prohibiting defendant from engaging in the alleged misconduct and such other equitable
24 relief as the court deems appropriate.

COUNT V
DECLARATORY RELIEF
(On Behalf of Plaintiff and the Nationwide Class)

160. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

161. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

162. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class Members' Private Information, as well as whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from future data breaches that compromise their Private Information. Plaintiff and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

163. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect employee and patient Private Information.

164. Defendant still possesses the Private Information of Plaintiff and the Class.

165. To Plaintiff's knowledge, Defendant has made no announcement that it has changed its data storage or security practices relating to the Private Information.

166. To Plaintiff's knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

167. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach. The risk of another such breach is real, immediate, and substantial.

1 168. The hardship to Plaintiff and Class Members if an injunction does not issue
 2 exceeds the hardship to Defendant if an injunction is issued. Among other things, if another
 3 data breach occurs at Convergent, Plaintiff and Class Members will likely continue to be
 4 subjected to fraud, identify theft, and other harms described herein. On the other hand, the
 5 cost to Defendant of complying with an injunction by employing reasonable prospective data
 6 security measures is relatively minimal, and Defendant has a pre-existing legal obligation to
 7 employ such measures.

8 169. Issuance of the requested injunction will not disserve the public interest. To the
 9 contrary, such an injunction would benefit the public by preventing another data breach at
 10 Convergent, thus eliminating the additional injuries that would result to Plaintiff and Class
 11 Members.

12 170. Pursuant to its authority under the Declaratory Judgment Act, this Court should
 13 enter a judgment declaring that Defendant implement and maintain reasonable security
 14 measures, including but not limited to the following:

- 15 a. Engaging third-party security auditors/penetration testers, as well as
 16 internal security personnel, to conduct testing that includes simulated
 17 attacks, penetration tests, and audits on Defendant's systems on a
 18 periodic basis, and ordering Defendant to promptly correct any problems
 19 or issues detected by such third-party security auditors;
- 20 b. engaging third-party security auditors and internal personnel to run
 21 automated security monitoring;
- 22 c. auditing, testing, and training its security personnel regarding any new or
 23 modified procedures;
- 24 d. purging, deleting, and destroying Private Information not necessary for
 25 its provisions of services in a reasonably secure manner;
- 26 e. conducting regular database scans and security checks; and
 27

- f. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Classes, and appointing Plaintiff and his Counsel to represent the Classes;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

- i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
- ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
- iii. requiring Defendant to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;
- v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures;
- ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- x. requiring Defendant to conduct regular database scanning and securing checks;
- xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

- xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
- xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

1 D. For an award of damages, including, but not limited to, actual, consequential,
2 and nominal damages, as allowed by law in an amount to be determined;

3 E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

4 F. For prejudgment interest on all amounts awarded; and

5 G. Such other and further relief as this Court may deem just and proper.

6 **VII. DEMAND FOR JURY TRIAL**

7 Plaintiff hereby demands that this matter be tried before a jury.

8 RESPECTFULLY SUBMITTED AND DATED this 3rd day of November, 2022.

9
10 TERRELL MARSHALL LAW GROUP PLLC

11 By: /s/Beth E. Terrell, WSBA #26759

Beth E. Terrell, WSBA #26759

Email: bterrell@terrellmarshall.com

13 By: /s/Ryan Tack-Hooper, WSBA #56423

Ryan Tack-Hooper, WSBA #56423

Email: rtack-hooper@terrellmarshall.com

16 Keith L. Gibson, *Pro Hac Vice Forthcoming*

Email: kgibson@terrellmarshall.com

936 North 34th Street, Suite 300

Seattle, Washington 98103

Telephone: (206) 816-6603

Facsimile: (206) 319-5450

20 Jean S. Martin, *Pro Hac Vice Forthcoming*

Email: jeanmartin@ForThePeople.com

Francesca Kester, *Pro Hac Vice Forthcoming*

Email: fkester@ForThePeople.com

22 MORGAN & MORGAN COMPLEX

LITIGATION GROUP

201 N. Franklin Street, 7th Floor

Tampa, Florida 33602

Telephone: (813) 223-5505

26 *Attorneys for Plaintiff and Putative Class*